UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
09/767,610	01/22/2001	Mark Moriconi	PA1677US	2724

23910 7590 07/27/2004

FLIESLER MEYER, LLP
FOUR EMBARCADERO CENTER
SUITE 400
SAN FRANCISCO, CA 94111

EXAMINER	
HOFFMAN, BRANDON S	

ART UNIT	PAPER NUMBER
2136	

DATE MAILED: 07/27/2004

Please find below and/or attached an Office communication concerning this application or proceeding.

Office Action Summary	Application No.	Applicant(s)	
	09/767,610	MORICONI ET AL.	
	Examiner	Art Unit	
	Brandon Hoffman	2136	

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE 3 MONTH(S) FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If the period for reply specified above is less than thirty (30) days, a reply within the statutory minimum of thirty (30) days will be considered timely.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

1)☐ Responsive to communication(s) filed on _____.

2a)☐ This action is **FINAL**. 2b)☒ This action is non-final.

3)☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

4)☒ Claim(s) *58-76,112-127,133-135 and 147-156* is/are pending in the application.

4a) Of the above claim(s) _____ is/are withdrawn from consideration.

5)☐ Claim(s) _____ is/are allowed.

6)☒ Claim(s) *58-70,72-76,112-127,133-135,147 and 149-156* is/are rejected.

7)☒ Claim(s) *71 and 148* is/are objected to.

8)☐ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

9)☐ The specification is objected to by the Examiner.

10)☒ The drawing(s) filed on *22 January 2001* is/are: a)☒ accepted or b)☐ objected to by the Examiner.

Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).

Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).

11)☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

12)☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).

a)☐ All b)☐ Some * c)☐ None of:

1.☐ Certified copies of the priority documents have been received.

2.☐ Certified copies of the priority documents have been received in Application No. _____.

3.☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

* See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

1) ☒ Notice of References Cited (PTO-892)
2) ☐ Notice of Draftsperson's Patent Drawing Review (PTO-948)
3) ☒ Information Disclosure Statement(s) (PTO-1449 or PTO/SB/08) Paper No(s)/Mail Date _____.
4) ☐ Interview Summary (PTO-413) Paper No(s)/Mail Date. _____.
5) ☐ Notice of Informal Patent Application (PTO-152)
6) ☐ Other: _____.

DETAILED ACTION

Election/Restrictions

1. Restriction to one of the following inventions is required under 35 U.S.C. 121:

   I. Claims 128-132, drawn to network distribution, classified in class 709, subclass 223.

   II. Claims 77-111 and 136-146, drawn to policy management, classified in class 705, subclass 1.

   III. Claims 58-76, 112-127, 133-135, and 147-156, drawn to security, classified in class 713, subclass 201.

The inventions are distinct, each from the other because of the following reasons:

Inventions I and II are related as subcombinations disclosed as usable together in a single combination. The subcombinations are distinct from each other if they are shown to be separately usable. In the instant case, invention II has separate utility such as defining rules that govern user access. See MPEP § 806.05(d).

Inventions II and III are related as subcombinations disclosed as usable together in a single combination. The subcombinations are distinct from each other if they are shown to be separately usable. In the instant case, invention III has separate utility such as keeping users secure over a distributed network. See MPEP § 806.05(d).

Inventions III and I are related as subcombinations disclosed as usable together in a single combination. The subcombinations are distinct from each other if they are

shown to be separately usable. In the instant case, invention I has separate utility such as a way to transfer data from one computer to another. See MPEP § 806.05(d).

Because these inventions are distinct for the reasons given above and have acquired a separate status in the art as shown by their different classification, restriction for examination purposes as indicated is proper.

2. An examiner's amendment to the record appears below. Should the changes and/or additions be unacceptable to applicant, an amendment may be filed as provided by 37 CFR 1.312. To ensure consideration of such an amendment, it MUST be submitted no later than the payment of the issue fee.

Authorization for this examiner's amendment was given in a telephone interview with Karl Kenna on July 9, 2004.

The application has been amended as follows: claims 1-57, which were previously statutory double patenting issues are now cancelled, claims belonging to group I, pertaining to network distribution, and claims belonging to group II, pertaining to policies, are now withdrawn. Accordingly, claims 58-76, 112-127, 133-135, and 147-156 are pending in this application.

Claim Rejections - 35 USC § 112

3. The following is a quotation of the second paragraph of 35 U.S.C. 112:

> The specification shall conclude with one or more claims particularly pointing out and distinctly claiming the subject matter which the applicant regards as his invention.

4. Claim 117 is rejected under 35 U.S.C. 112, second paragraph, as being indefinite for failing to particularly point out and distinctly claim the subject matter which applicant regards as the invention.

Claim 117 recites the limitation "the authorization engine" in line 1. There is insufficient antecedent basis for this limitation in the claim.

Claim Rejections - 35 USC § 102

5. The following is a quotation of the appropriate paragraphs of 35 U.S.C. 102 that form the basis for the rejections under this section made in this Office action:

> A person shall be entitled to a patent unless –
>
> (e) the invention was described in (1) an application for patent, published under section 122(b), by another filed in the United States before the invention by the applicant for patent or (2) a patent granted on an application for patent by another filed in the United States before the invention by the applicant for patent, except that an international application filed under the treaty defined in section 351(a) shall have the effects for purposes of this subsection of an application filed in the United States only if the international application designated the United States and was published under Article 21(2) of such treaty in the English language.

6. Claims 58-70, 72-74, 112-114, 118, 119, 121-127, and 149-156 are rejected under 35 U.S.C. 102(e) as being anticipated by Nessett et al. (U.S. Patent No. 5,968,176).

Regarding claim 58, Nessett et al. teaches a system for maintaining security in a distributed computing environment comprising:

- A policy manager for managing a security policy (fig. 1 and col. 3, lines 58-67); and

- An application guard for managing access to a transaction related with an application as specified by the security policy (col. 7, lines 4-12 and col. 8, lines 39-55).

Regarding claim 59, Nessett et al. teaches a system for managing and enforcing complex security requirements to protect computer systems against unauthorized access in a distributed computer network comprising:

- A policy manager located on a server for managing and distributing a policy to a client (fig. 1 and col. 3, lines 58-67); and
- An application guard located on the client, acting to grant or deny access to various components of the client, as specified by the policy (col. 7, lines 4-12 and col. 8, lines 39-55).

Regarding claim 60, Nessett et al. teaches wherein the server is connected via a network to the client (fig. 1, ref. num 10).

Regarding claim 61, Nessett et al. teaches wherein the server is connected to many clients (fig. 1, ref. num 11 and 12-16).

Regarding claim 62, Nessett et al. teaches the server further comprising a central processing unit, a Read-only Memory (ROM), a Random-Access Memory, a non-volatile memory, an input device, and a display, wherein the ROM, the RAM, non-volatile

memory, input device and display are connected via a bus (col. 6, lines 64-66, a well-known server as understood in the technology has all of these components connected by a bus.).

Regarding claims 63 and 72, Nessett et al. combined with inherency teaches wherein the policy manager is a program located on a server in non-volatile memory (col. 6, lines 64-66, it is inherent that the program is stored on the server in non-volatile memory).

Regarding claim 64, Nessett et al. teaches wherein the client contains a program stored in non-volatile memory for granting or denying access to various components or resources of the client, as specified by the policy distributed from the server (col. 7, lines 4-12 and col. 8, lines 39-55).

Regarding claim 65, Nessett et al. teaches wherein the server includes a non-volatile memory storing the policy manager that specifies the security requirements for applications and database objects (fig. 1 and col. 3, lines 58-67); said policy contains security rules that describe at least one constraint that constrains which applications a particular user can access and which objects within an application a user can access (col. 8, lines 39-55).

Regarding claim 66, Nessett et al. teaches wherein the policy manager allows the administrator to choose whether the constraints are affected by any of time, geography, and external events (col. 8, lines 43-46 and 51-54 [external is at a different geographical location]).

Regarding claim 67, Nessett et al. teaches wherein the policy is capable of constraining access to applications and operations within applications (col. 8, lines 50-51 [audit is an operation within an application]).

Regarding claim 68, Nessett et al. teaches wherein the policy is organized into groups and hierarchies (fig. 7, ref. num 600 and 610 and col. 8, lines 48-54).

Regarding claim 69, Nessett et al. teaches wherein the policy includes access rules, which include:

- A grant rule that grants a privilege to a subject on an object under a first constraint (col. 8, lines 40-54, under *Policy Statement*, ALLOW); and
- A deny rule that denies a privilege to a subject on an object under a second constraint (col. 8, lines 40-54, under *Policy Statement*, DISALLOW).

Regarding claim 70, Nessett et al. teaches the policy manager further comprises a management station program to operate the policy manager, a distributor program to distribute local client policies to clients, a logger program to track authorization requests,

and a database management system (DBMS) to maintain policy data files (fig. 1, ref. num 11, col. 6, lines 12-34, col. 9, lines 7-11, and col. 13, lines 32-38).

Regarding claim 73, Nessett et al. teaches wherein the policy manager allows system users to implement, analyze, edit and update a centrally managed policy (col. 5, lines 51-56 and col. 13, lines 32-38).

Regarding claim 74, Nessett et al. teaches wherein the policy includes at least one policy rule comprising:

- An object that is to be protected (col. 8, lines 40-54, "ACTIVITY);
- An access right or privilege (col. 8, lines 40-54, "POLICY STATEMENT");
- A global or local user to which the privilege applies (col. 8, lines 40-54, "DESTINATION); and
- Conditions under which the privilege is granted or denied, wherein the user is given a choice of types of conditions including
    - Whether to use built-in access criteria wherein the user can select whether to use time of day and whether to use location (col. 8, lines 27-33), and
    - Whether to use custom-defined access criteria (col. 7, lines 41-45).

Regarding claim 112, Nessett et al. teaches a security system comprising at least one application guard that is stored on a computer readable medium and that guards a

protected application by preventing unauthorized transactional access to at least a portion of said application (col. 7, lines 4-12 and col. 8, lines 39-55).

Regarding claim 113, Nessett et al. teaches a security system comprising an application guard located within non-volatile memory that is designed to reside along with each protected application and supports transactional access control by allowing an application to detect an authorization service and to make authorization requests at each user interaction, data request, and business-level transaction (col. 7, lines 4-12 and col. 8, lines 39-55).

Regarding claim 114, Nessett et al. teaches further comprising a distributor capable of distributing the application guard to client located throughout an enterprise (col. 7, lines 31-35).

Regarding claim 118, Nessett et al. teaches further comprising a logger where at least:

- Each authorization request is recorded in an audit log (col. 13, lines 32-38); and
- Each authorization request made at a location remote from the logger is transmitted via a communication interface to the logger (col. 13, lines 32-38 and fig. 1, ref. num 13 and col. 10, lines 41-43).

Regarding claim 119, Nessett et al. teaches wherein the system is capable of implementing at least:

- The application guard locally to the application (col. 7, lines 4-12); and
- The application guard as a remote authorization service through a remote procedure call to another server (col. 7, lines 4-12 and fig. 1, ref. num 13 and col. 10, lines 41-43).

Regarding claim 121, Nessett et al. teaches a computer readable storage medium having stored thereon a method for maintaining security in a distributed computing environment comprising the steps of:

- Managing a security policy via a policy manager (fig. 1 and col. 3, lines 58-67); and
- Managing access via an application guard to a transaction related with an application as specified by the security policy (col. 7, lines 4-12 and col. 8, lines 39-55).

Regarding claim 122, Nessett et al. teaches a method for maintaining security in a distributed computing environment comprising:

- Managing a security policy via a policy manager (fig. 1 and col. 3, lines 58-67); and

- Managing access via an application guard to a transaction referenced by an application as specified by the security policy (col. 7, lines 4-12 and col. 8, lines 39-55).

Regarding claim 123, Nessett et al. teaches a method of using a security system comprising:

- Using a management station, including a communication interface, to create or modify a policy rule (fig. 1, ref. num 11 and col. 7, lines 36-45); and
- Distributing the policy rule to appropriate clients via the communication interface (fig. 1, ref. num 10 and col. 7, lines 31-35).

Regarding claim 124, Nessett et al. teaches further comprising reviewing and reconstructing the policy rules via a parser to make sure that the policy rules are syntactically and semantically correct according to a predefined policy language (col. 7, lines 41-45).

Regarding claim 125, Nessett et al. teaches further comprising determining via a differ-program the changes that were made to optimize the policy, and wherein the step of distributing then distributes only the changed policy rules or local client policy to the appropriate application guards, which enforce access control to local applications and data (col. 5, lines 51-57).

Regarding claim 126, Nessett et al. teaches wherein each application guard has its own specific local client policy (col. 5, lines 45-47).

Regarding claim 127, Nessett et al. teaches further comprising optimizing via the distributor an administrative policy into an optimized administrative policy or local administrative policy for use with an application guard in the management station (col. 5, lines 51-57 and col. 7, lines 31-35).

Regarding claim 149, Nessett et al. teaches a method for securing a computer system, comprising guarding a protected application by using an application guard to prevent unauthorized transactional access (col. 7, lines 4-12 and col. 8, lines 39-55).

Regarding claim 150, Nessett et al. teaches a method for providing a security system, comprising providing at least one application guard that is storable on a computer readable medium and guards a protected application by preventing unauthorized transactional access to at least a component associated with the application (col. 7, lines 4-12 and col. 8, lines 39-55).

Regarding claim 151, Nessett et al. teaches a method for updating a security system, comprising:

- Updating a set of policy rules containing at least one policy rule in a central location (col. 7, lines 36-47);

- Generating changes to the set of policy rules resulting from the updating step (col. 5, lines 51-57); and
- Distributing the changes (col. 5, lines 51-57).

Regarding claim 154, Nessett et al. teaches a method for establishing a security system, comprising:

- Establishing a set of policy rules containing at least one policy rule in a central location (col. 7, lines 36-47); and
- Distributing the set of policy rules for enforcement (col. 7, lines 31-35).

Regarding claims 152 and 155, Nessett et al. teaches wherein the policy rule contains entitlement information related to at least one resource (col. 8, lines 40-54).

Regarding claims 153 and 156, Nessett et al. teaches wherein the policy rules are stored in a database table (fig. 1, ref. num 30 and col. 7, lines 13-21).

Claim Rejections - 35 USC § 103

7. The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all obviousness rejections set forth in this Office action:

> (a) A patent may not be obtained though the invention is not identically disclosed or described as set forth in section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains. Patentability shall not be negatived by the manner in which the invention was made.

8. Claims 76, 115, and 120 are rejected under 35 U.S.C. 103(a) as being unpatentable over Nessett et al. (U.S. Patent No. 5,968,176) in view of Klein et al. (U.S. Patent No. 6,539,414).

Regarding claim 76, Nessett et al. teaches all the limitations of claim 59 above. However, Nessett et al. does not teach wherein the policy manager comprises an Application Programming Interface (API) that at least allows programs to perform the same functions as a human operator.

Klein et al. teaches wherein the policy manager comprises an Application Programming Interface (API) that at least allows programs to perform the same functions as a human operator (fig. 1, ref. num 50 and col. 4, lines 54-66).

It would have been obvious to one of ordinary skill in the art, at the time the invention was made, to combine the policy manage comprising an API to allow the programs to perform functions the same as a human operator, as taught by Klein et al., with the system of Nessett et al. It would have been obvious for such modifications, as taught by Klein et al., with the system of Nessett et al. because an automated policy manager allows less human-to-computer interfacing, thereby saving time and money for managing a system.

Regarding claim 115, Nessett et al. teaches all the limitations of claim 113 above. However, Nessett et al. does not teach wherein the application guard is coupled to the application through an application programming interface (API) or authorization library that allows the application to request authorization services as needed through an application guard interface.

Klein et al. teaches wherein the application guard is coupled to the application through an application programming interface (API) or authorization library that allows the application to request authorization services as needed through an application guard interface (fig. 1, ref. num 50 and col. 4, lines 54-66).

It would have been obvious to one of ordinary skill in the art, at the time the invention was made, to combine the application guard is coupled through an API to allow requests for authorization services, as taught by Klein et al., with the system of Nessett et al. It would have been obvious for such modifications, as taught by Klein et al., with the system of Nessett et al. because an automated policy manager allows less human-to-computer interfacing, thereby saving time and money for managing a system.

Regarding claim 120, Nessett et al. teaches a security system comprising:

- At least one application guard stored on a computer readable non-volatile memory medium that is designed to reside along with each protected application and guards a protected application by preventing unauthorized transactional

access, and supports transactional access control by allowing an application to detect an authorization service and to make authorization requests at each user interaction, data request, and business-level transaction (col. 7, lines 4-12 and col. 8, lines 39-55);

- The system is capable of implementing the application guard locally to the application and is capable of implementing the application guard as a remote authorization service through a remote procedure call to another server (col. 7, lines 4-12 and fig. 1, ref. num 13 and col. 10, lines 41-43).

Nessett et al. does not teach wherein the application guard is integrated into the application through an application programming interface (API) or authorization library that allows the application to request authorization services as needed through an application guard interface.

Klein et al. teaches wherein the application guard is integrated into the application through an application programming interface (API) or authorization library that allows the application to request authorization services as needed through an application guard interface (fig. 1, ref. num 50 and col. 4, lines 54-66).

It would have been obvious to one of ordinary skill in the art, at the time the invention was made, to combine the application guard is integrated into the application through an API or authorization library that allows the application to request

authorization services as needed through an application guard interface, as taught by Klein et al., with the method of Nessett et al. It would have been obvious for such modifications, as taught by Klein et al., with the method of Nessett et al. because an automated policy manager allows less human-to-computer interfacing, thereby saving time and money for managing a system.

Claims 117 and 133-135 are rejected under 35 U.S.C. 103(a) as being unpatentable over Nessett et al. (U.S. Patent No. 5,968,176) in view of Brooks et al. (U.S. Patent No. 6,009,507).

Regarding claim 117, Nessett et al. teaches all the limitations of claim 113 above. However, Nessett et al. does not teach wherein the authorization engine comprises plug-ins that at least allow for additional capabilities to process and evaluate authorization requests based on customized code.

Brooks et al. teaches wherein the authorization engine comprises plug-ins that at least allow for additional capabilities to process and evaluate authorization requests based on customized code (col. 6, lines 26-36).

It would have been obvious to one of ordinary skill in the art, at the time the invention was made, to combine registering plug-ins into the application guards to allow for additional capabilities in order to process authorization requests based on

customized code, as taught by Brooks et al., with the system of Nessett et al. It would have been obvious for such modifications, as taught by Brooks et al., with the system of Nessett et al. because the plug-ins allow for maximum CPU usage, therefore getting the most processing power available from each client in a centrally managed security policy.

Regarding claim 133, Nessett et al. teaches a method of configuring a security system comprising:

- Installing a policy manager on a server including installing a management station, a distributor, a logger, and a Database Management System (DBMS) (fig. 1, ref. num 11, col. 6, lines 12-34, col. 9, lines 7-11, and col. 13, lines 32-38);
- Entering a set of policy rules (col. 7, lines 22-35); and
- Installing application guards and local client policies onto client systems (col. 7, lines 4-12 and 31-35 and col. 8, lines 39-55).

Nessett et al. does not teach registering plug-ins into the application guards to allow for additional capabilities in order to process authorization requests based on customized code.

Brooks et al. teaches registering plug-ins into the application guards to allow for additional capabilities in order to process authorization requests based on customized code (col. 6, lines 26-36).

It would have been obvious to one of ordinary skill in the art, at the time the invention was made, to combine registering plug-ins into the application guards to allow for additional capabilities in order to process authorization requests based on customized code, as taught by Brooks et al., with the method of Nessett et al. It would have been obvious for such modifications, as taught by Brooks et al., with the method of Nessett et al. because the plug-ins allow for maximum CPU usage, therefore getting the most processing power available from each client in a centrally managed security policy.

Regarding claim 134, the combination of Nessett et al. in view of Brooks et al. teaches wherein the step of entering includes presenting an administrator with the choice of whether to use a policy loader or a management station to enter the policy rules (see col. 7, lines 36-47 of Nessett et al.).

Regarding claim 135, the combination of Nessett et al. in view of Brooks et al. teaches wherein:

- If the administrator chooses to use the management station, then the step of entering includes using an edit function to enter the policy rules (see col. 7, lines 38-41 of Nessett et al.), and

- If the administrator chooses to use the policy loader, then the step of entering includes entering the policy rules into a file, and passing the file to the policy loader (see col. 7, lines 36-38 of Nessett et al.).

Double Patenting

9. The nonstatutory double patenting rejection is based on a judicially created doctrine grounded in public policy (a policy reflected in the statute) so as to prevent the unjustified or improper timewise extension of the "right to exclude" granted by a patent and to prevent possible harassment by multiple assignees. See *In re Goodman*, 11 F.3d 1046, 29 USPQ2d 2010 (Fed. Cir. 1993); *In re Longi*, 759 F.2d 887, 225 USPQ 645 (Fed. Cir. 1985); *In re Van Ornum*, 686 F.2d 937, 214 USPQ 761 (CCPA 1982); *In re Vogel*, 422 F.2d 438, 164 USPQ 619 (CCPA 1970);and, *In re Thorington,* 418 F.2d 528, 163 USPQ 644 (CCPA 1969).

A timely filed terminal disclaimer in compliance with 37 CFR 1.321(c) may be used to overcome an actual or provisional rejection based on a nonstatutory double patenting ground provided the conflicting application or patent is shown to be commonly owned with this application. See 37 CFR 1.130(b).

Effective January 1, 1994, a registered attorney or agent of record may sign a terminal disclaimer. A terminal disclaimer signed by the assignee must fully comply with 37 CFR 3.73(b).

10. Claims 75, 116, and 147 are rejected under the judicially created doctrine of double patenting over claims 1, 4, 5, 9, 13, 14, 47, 50, and 52 of U. S. Patent No. 6,158,010 since the claims, if allowed, would improperly extend the "right to exclude" already granted in the patent.

The subject matter claimed in the instant application is fully disclosed in the patent and is covered by the patent since the patent and the application are claiming common subject matter, as follows: a policy manager for managing a policy, an application guard located on the client for managing access to applications as specified by the policy, an authorization engine for evaluating authorization requests, the engine

can either deny or allow the requests, a logger for logging the authorization requests, a menu with the navigate, analyze, edit, distribute, & view audit log features,

Furthermore, there is no apparent reason why applicant was prevented from presenting claims corresponding to those of the instant application during prosecution of the application which matured into a patent. See *In re Schneller*, 397 F.2d 350, 158 USPQ 210 (CCPA 1968). See also MPEP § 804.

Allowable Subject Matter

11. Claims 71 and 148 are objected to as being dependent upon a rejected base claim, but would be allowable if rewritten in independent form including all of the limitations of the base claim and any intervening claims.

Any inquiry concerning this communication or earlier communications from the examiner should be directed to Brandon Hoffman whose telephone number is 703-305-4662. The examiner can normally be reached on M-F 8:30 - 5:00.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Ayaz Sheikh can be reached on 703-305-9648. The fax phone number for the organization where this application or proceeding is assigned is 703-872-9306.

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see http://pair-direct.uspto.gov. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free).

Brandon Hoffman

BH

AYAZ SHEIKH
SUPERVISORY PATENT EXAMINER
TECHNOLOGY CENTER 2100